UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/721,942	11/27/2000	Ulf Mattsson	0104-0310P	4284

26161 7590 10/19/2005

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DINH, MINH	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/721,942	MATTSSON ET AL.	
	Examiner	Art Unit	
	Minh Dinh	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the reply filed 08/01/2005.

Response to Arguments

2. Applicant's arguments filed 08/01/2005 have been fully considered but they are not persuasive. Applicant argues that Morar (6,678,822) does not disclose reading a data type of a data element but only discloses guessing a data type of a data element by reading a string, analyzing the content of the string and inferring the data type of the string (page 1, last paragraph). Neither claim 1 nor claim 7 recites how the step of reading a data type is done; therefore, the limitation "reading a data type" is interpreted as "receiving/getting the data type" which Morar teaches. Applicant argues that Morar uses a "restricting word set" but not a "restricting character set" and, as a result, Morar encryption is performed by replacing one whole word with another word possibly of different length as opposed to replacing each character with a character in the restricting character set as claimed (page 2). Morar discloses replacing each numeric digit with a digit (col. 9, lines 9-14). In this case, a "restricting character set" (i.e., digits) is used and replacement is performed for each digit.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3 and 7-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Morar et al (6,678,822).

Regarding claims 1 and 7, Morar discloses a method for encrypting restricted information in a database, the method comprising: reading a data type of a first data element; interpreting said data type to form a restricting character set; and encrypting each character of said first data element into an encrypted character selected from said restricting character set (col. 1, lines 36-46; col. 4, lines 7-12; col. 8, line 55 – col. 9, line 14; col. 11, lines 37-58).

Regarding claim 2, Morar further discloses processing character-based information (col. 9, lines 9-14; col. 11, lines 53-58). Inherently, characters of a character set are arranged in a pattern for a data type so that a data type such as number can be recognized.

Regarding claim 3, Morar further discloses the encryption results in a data element having the same number of characters as the unencrypted data element (col. 9, lines 9-14).

Regarding claims 8-11, Morar further discloses that the encryption is performed on a working copy of a database and that the encrypted characters are stored in the data element replacing the plaintext characters (col. 8, line 41 – col. 9, line 14).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morar as applied to claim 1 above, and further in view of Schneier ("Applied Cryptography").

Regarding claim 4, Morar further discloses replacing characters of a data element with random characters of the same data type (col. 9, lines 9-14; col. 11, lines 53-58). Inherently, each character is assigned an index value. However, Morar does not disclose adding a varying value to each index value before encryption. Schneier discloses an encryption method called one-time pad including the steps of converting each character to an index value and adding a varying value to each index value before encryption (Section 1.5, page 15). It would have been obvious to one of ordinary skill in the ad at the time the invention was made to modify the Morar method of to include the step of adding a varying value to each index value before encryption, as taught by Schneier. The one-time pad is a perfect encryption scheme.

Regarding claim 6, Morar does not disclose using the DES algorithm in stream cipher mode. Schneier discloses using the DES algorithm in CFB mode of operation, which meets the limitation of DES algorithm in stream cipher mode (Section 12.2, page

277, see Modes of DES). It would have been obvious to one of ordinary skill in the ad at the time the invention was made to modify the Morar method to use the DES algorithm in stream cipher mode. The motivation for doing so would have been that the 8-bit CFB is generally the mode of choice for encrypting stream of characters when each character has to be treated individually (Section 9.1 1, page 210).

7. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Morar in view of Schneier as applied to claim 4 above, and further in view of Marshall et al. (4,866,707).

Morar and Schneier (Section 1.5) do not disclose adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character. Schneier, in Section 9.3, discloses a cipher block chaining (CBC) mode in which adjacent blocks are XORed pairwise from the left to the right using an initialization vector with the leftmost unit (page 194, fig. 9.3 and "Prevent this by encrypting ... use some random bits from someplace"); the teaching of Schneier reads on the adding step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Morar and Schneier (Section 1.5) to include the step of adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character, as taught by Schneier (Section 9.3). The motivation for doing so would have been that the ciphertext block is dependent not just on the plaintext block that generated it but on all the previous plaintext blocks (page 193).

Morar and Schneier do not disclose creating an initial value by hashing the encryption key. Marshall discloses a CBC encryption technique including the step of creating an initialization vector by encrypting a message key (col. 9, lines 13-19); the teaching of Marshall reads on the creating step of the claim. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify combined method of Morar and Schneier to include the step of creating an initial value by hashing the encryption key, as taught by Marshall. The motivation for doing so would have been that the same message being sent a second time would be encrypted under a different key, so an outsider would not be able to gain much assistance from the repetition in trying to breach the encryption (col. 9, lines 27-33).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,950,518 to Henson et al.

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
10/08/2005

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100